The Interim Years of Cyberspace

Robert M. Lee, 1st Lieutenant, USAF

There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success than to take the lead in the introduction of a new order of things.

— Machiavelli

In the early years of the cyberspace domain the role of cyberpower was primarily seen as a means to achieve broad command and control across the warfighting domains. Communication was the key focus of the domain and ensuring the lines of communication were maintained was imperative to operational success. As the domain grew, additional roles were edged out to provide a support force to traditional military operations while other roles were explored with the highest levels of secrecy. Many early cyberspace leaders realized that cyber assets offered a number of attack, defense, and exploitation options that have never before been afforded to military commanders. In a highly connected world with large advancements in technology common, the capabilities and weapons in cyberspace became even more impressive.

The current stage of cyberspace development is similar to the interim years between World War I and World War II when airpower was challenged and emerged as a premier and powerful military tool. No comparison does better justice to the current situation in cyberspace than airpower during those foundational years. It was during airpower's early years that theorists and military officers including Italian Air Marshall Giulio Douhet, Marshal of the Royal Air Force Hugh Trenchard, and Brigadier General William "Billy" Mitchell helped guide the direction of airpower. Through a focus on sharing actionable cyber-intelligence, showcasing select cyber capabilities, embracing the development of the cyber culture, and dedicating a large focus on education, the direction of cyberpower can be equally guided. As cyberspace reaches its full potential as a domain of warfare equal to the traditional domains it is imperative that it be vectored properly.

The Interim Years of Airpower

Previous to World War I the use of aircraft was extremely limited and many did not see it as a viable military option. As an example, William H. Pickering stated in his 1908 book *Aeronautics* that "another popular fallacy is to suppose that flying machines could be used to drop dynamite on an enemy in a time of war." Yet only six years later on 14 August 1914 a French Voisin aircraft was used to bomb German zeppelin hangers at Metz-Frascaty.[1] The idea that aerial warfare could be used in combat quickly gained prominence. Over the next few years strategic bombing aircraft were developed and used in air raids including

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Interim Years of Cyberspace	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Research Institute (AFRI) ,155 N. Twining Street,Maxwell AFB,AL,36112**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Air & Space Power Journal. Volume 24, Number 3, 2012

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**17**	

the German Gotha Raids on England.[2] However, the concept of using aircraft and balloons in warfare was not a new idea. One of the earliest uses dates back to 3rd century China where General Zhuge Liang used Kongming Lanterns to signal military forces and scare away enemies.[3] Yet, it took advancements in technology and powerful demonstrations of force in World War I to expedite the domain's importance and use.

With the success of airpower in World War I, to include Lieutenant Frank Luke Jr.'s destruction of fourteen heavily guarded German balloons,[4] it was obvious to many military leaders that aircraft could serve a support role to the traditional domains of land and naval warfare. The debate at the time was not over if airpower would be used, but how it would be developed and which branch of service would take the lead. In the years between World War I and World War II the focus of aviation was on providing defense from adversaries.[5] The focus on defense was an important one but some of the aerial defensive capabilities also offered offensive possibilities. The flexibility of airpower created intense debates between the Army and Navy due to the fact that Army Air Corps aircraft could fill roles that the Navy traditionally maintained.

In 1921 General William "Billy" Mitchell conducted a test where he attempted to sink naval vessels with his MB-2 bombers from Langley Field, Virginia. His mission was a success and the bombers sank three naval vessels used for the test including a modern battleship captured from the Germans named the Ostfriesland.[6] General Mitchell's test showed that aircraft could act independently to attack offshore targets. It also demonstrated that if the Army continued to empower their Air Corps the Navy might lose the primary responsibility of providing coastal defense.

In 1925, partially in rebuttal to General Mitchell's test against the Ostfriesland, the Navy revealed a plan to increase their shore-based aircraft from 334 planes to 583.[7] The Air Service Chief Major General Mason Patrick felt that this was a move by the Navy Department to take control over the entire coastal defense mission.[8] The fight between the Army and Navy continued to escalate and leaders of both services worried that if a solution could not be met that Congress might make an independent air corps.[9] The conflict continued though despite intervention by the War Department and Congress in attempts to satisfy both services.[10] Amidst the services' disagreement, General Mitchell strongly advocated that a separate branch of service was needed. He turned to the public to make statements and win their support in an effort to pressure Congress to act.[11] After General Mitchell's court-martial he resigned in 1926 from the U.S. Army Air Service and continued to publically campaign for an independent Air Force.[12]

In 1934, General Henry "Hap" Arnold was tasked to fly from Dayton, Ohio to Alaska with ten Martin B-10 bombers. On the return trip to Ohio he

detoured from his route by flying a section of the journey over the ocean instead of across Canada. This demonstrated the bombers' coastal range and in doing so enraged the Army Chief of Staff Gen Douglas MacArthur.[13] It was starting to become apparent to members of Congress and the War Department that a separate branch of service may be needed. General Mitchell and other proponents of airpower continued to advocate for this separate branch.[14] The actions of key members such as General Arnold and General Mitchell helped lead to an independent Air Force, but such actions are not needed in the cyberspace domain. However, the lessons learned from the development of the aerial domain offer key insights into effective strategies for cyberspace domain development.

Lessons Learned from Airpower

The cyberspace domain does not encroach on traditional roles of the Army, Air Force, or Navy. The cyber mission has the ability to work both independently from, and synergistically with, the traditional warfighting domains across each branch. Cyberpower is also able to provide support to national defense, intelligence gathering capabilities, and offensive actions equal or greater to other military actions. However, the idea that cyber capabilities alone can win a war is limited thinking. Cyberpower, very much like airpower, can be a destructive power if wielded alone and to its full measure. Early Airmen took pride in believing that aerial attacks alone could lead to victory at war; they did not understand how destructive it could be if left unchecked though and the importance of limiting conflict.[15] Likewise, cyber enthusiasts must embrace cyberpower but in its true capability as a component of combined military force.

During the Vietnam War President Lyndon Johnson and Secretary of Defense Robert McNamara met weekly to discuss the targets that pilots would bomb. Once thought to be political micromanagement, the real purpose of handpicking targets was to control the political implications that aerial attacks presented.[16] The new, and in many cases frightening, power brought by bombing raids was a strong statement not only to the North Vietnamese but to other nations watching closely. Cyberpower too has the ability to make influential statements and cannot be wielded lightly. A cyber attack that destroys an aircraft, disables a naval warship, or crashes the stock market will have enormous consequences to the political scene. Not only are these types of attacks powerful but they can be launched from anywhere in the world.

Italian Air Marshall Douhet thought that the range of aircraft would make it so that civilians and combatants alike would be targeted in future wars. Airpower, he reasoned, did not know the limits of traditional battlefields and could act uninhibited. No areas would feel safe to civilians without

boundaries on the battlefield.[17] In this same way, cyberpower's ability to quickly and specifically target networks and information systems throughout the world blurs the lines of battlefields. It is this characteristic in conjunction with its destructive force that causes a level of fear to surround cyber capabilities. The feeling in the population that they can be instantly impacted by cyber attacks can be as powerful as the fear that surrounds terrorist attacks. That feeling cannot be underestimated in its power to influence popular opinions and politics as well as its ability to guide the direction of cyber capability development. Cyberpower must always be one of many political tools at the disposal of military commanders and civilian leaders. It must never be the sole object of war.

The idea that technology will eliminate the ugly nature of war is one that has influenced military planners throughout the history of war.[18] Air Marshall Douhet believed that the inherently offensive nature of airpower, later famously reinforced by Sir Stanley Baldwin's statement that "the bomber will always get through,"[19] would limit the bloodshed during war. He believed that bombing cities and attack civilians would result in fewer deaths than the clashing of armies and resulting casualties of war.[20] Air Marshall Douhet's view that the morale of civilians would be broken with the introduction of strategic bombing was wrong. He believed this style of attack would cause civilians to demand their leaders to end wars early. Instead, aerial bombing raids usually bolstered civilian morale against the known enemy.[21] The issue in cyberspace is that without proper attribution the enemy may not be known. This could create unknown effects on the civilian population to include a broken morale similar to what Air Marshall Douhet had originally predicted. Regardless of the effects of an unknown cyber attacker, Air Marshal Douhet will continue to be wrong about technology's ability to end bloodshed. Technology must be researched and new advances made both in cyberspace and in the traditional warfighting domains, but the nature of war will always prevail; war is an ugly thing.[22]

General Mitchell's idea on airpower was notably different from Air Marshall Douhet's philosophies in that General Mitchell did not believe in targeting civilians. Instead, he believed it was effective to target infrastructure and industry sectors to limit the capabilities of the adversary. He also did not hold the belief that bombers were the quintessential form of airpower. General Mitchell believed that multiple types of aircraft were needed including those with offensive and reconnaissance focused missions.[23] General Mitchell's concept of airpower is more akin to the current diverse nature of cyberpower and varied assets. Furthermore, having multiple types of aircraft enabled the development of persistent intelligence, surveillance, and reconnaissance (ISR) aerial platforms and offensive air capabilities which help ensure air dominance and support to other warfighting domains.[24] The addition of varied types of cyberspace capabilities provides a direct increase to already established ISR and offensive operations while enabling the development of new operations.

Commanders and Actionable Cyber Intelligence

Cyberpower offers critical advantages to campaign planning. To offer commanders timelier options it is beneficial for offensive cyber operations to exist in the preparation of the operational environment phase. This phase includes compromising enemy networks and readying cyber weapons for use in the event of a conflict. While posturing for offensive cyber operations, information may be exploited from compromised systems and aid in the Joint Intelligence Preparation of the Operational Environment (JIPOE).[25] Through this gathered information commanders have more battlefield situational awareness.

Campaign planning is used by commanders to "synchronize efforts" and put forth complementing guidance.[26] The two major phases of the planning process, contingency planning and crisis action planning, benefit from the timely information and attack options which cyberpower presents. When the assumptions and plans made in the contingency phase more closely match the crisis action phase the Joint Operation Planning Process (JOPP) is expedited.[27] This quick selection process empowers Commanders with the ability to strike first, target precisely, and be more readily able to defend counter attacks. The information gathered from the preparation of the operational environment phase also decreases the effectiveness of enemy deception attempts.

With access to military doctrine, enemy forces may choose to avoid efficient or even fake, and otherwise appealing, courses of action (CoAs). The combination of cyber and ISR capabilities can detect these deceptions. The multiple ISR platforms such as manned aircraft, remotely piloted aircraft (RPAs), satellites, and human gathered intelligence contribute to the creation of the intelligence preparation of the battlespace (IPB).[28] Individually, cyber and ISR severely weaken the enemy's ability to hide troops, sensitive information, operational plans, and centers of gravity (CoGs). The combination of the two through Imagery Intelligence (IMINT), Signals Intelligence (SIGINT), Human Intelligence (HUMINT), and Computer Network Operations (CNO) provides an unprecedented level of battlefield situational awareness to commanders. This situational awareness can also enable cyberspace operations which provide capabilities to include weapon systems platforms that degrade, disrupt, and destroy adversary communication, control, and physical assets.

The situational awareness that cyber and ISR provides to commanders aids in setting forth holistic and realistic commander intent statements as discussed in the JOPP model. Through the creation of better commander intent statements the commander's planning guidance will be more accurate and assist in the selection of better CoAs.[29]

Never before have such capabilities been presented to the military planning process. These options are presented throughout the entirety of military operations and minimize the uncertainty of war that Carl von Clausewitz referred to as the fog of war.[30] Through more accurate planning and timely cyber offensive and defensive operations the chance for operational success is higher than ever before while also limiting the human and financial costs of war.

These cyber capabilities have not gone unnoticed though and the standup of U.S. Cyber Command indicated that the cyberspace domain is moving in the right direction.[31] However, more action was, and is, still needed to provide Commander's actionable intelligence and capabilities through cyber operations. Major General Brett T. Williams outlined his view for the direction of cyberspace in his "10 Propositions Regarding Cyberspace Operations." In the paper, Major General Williams stated that Joint Force Commander's and COCOMs needed to be empowered with cyber capabilities and C2 of cyber operations. Without visibility on components of cyber critical to a mission's success, Commanders are at a disadvantage. Major General Williams suggested the creation of the Theater Cyber Operations Command, similar to a Theater Special Operations Command, to provide geographic combatant commanders with cyber capabilities under the control of COCOMs.[32] The ability for commanders to request cyber capabilities relevant to their mission and have the cyber situational awareness to accurately do so is one of the most critical components of leveraging cyberpower.

This aspect of leveraging cyberpower effectively in COCOMs has gained attention since Major General William's paper. In the summer of 2011 General Keith Alexander, head of U.S. Cyber Command, discussed progress made in supporting operations in Iraq and Afghanistan through the deployment of expeditionary teams. He went on to reveal that progress has been made in supporting operational planning by the combatant commanders through an increased ability for them to request cyber support.[33]

There is much work to be done in the cyberspace domain to further provide cyber intelligence and capabilities to commanders. One of the issues pertaining to this is the classification of the information. To protect cyber capabilities it is important to not reveal certain details and technologies, doing so would allow adversaries to counter or safeguard against them. However, the intelligence and information gathered from cyber capabilities is currently over classified. Many commanders simply do not know all of what is available and thus cannot request those capabilities. Instead of only providing processes to request cyber requirements there must be a real effort made to declassify cyber intelligence and information that does not weaken cyber capabilities. This will not only support commanders but also empower tactical level leaders so that reasonable requests can be made to their leadership in support of daily operations. Moreover, the declassification of some cyber intelligence and

information would allow more sharing between government agencies and civilian leadership who operate in law enforcement agencies. Possibly even more important, the sharing of actionable cyber intelligence that could assist network defenses would enable civilian leadership to better protect sectors such as critical infrastructure. This sharing of information would lead to a direct correlation in increased national security.

Cyber Weapons and the Home Front

In June 2010 the Stuxnet worm was discovered and quickly gained notoriety as one of the most advanced pieces of malware ever discovered. The worm, a piece of malware that self-replicates and spreads between information systems, took advantage of an unprecedented four unpatched vulnerabilities, known as zero day vulnerabilities, while employing the first ever

programmable logic controller (PLC) rootkit, or piece of code that enables persistent access, while leveraging the use of two command and control servers and legitimate signed certificates.[34] The weapon system part of this cyber weapon was impressive but paled in comparison to the advanced nature of the payload portion.

Stuxnet was specifically designed to target supervisory control and data acquisition (SCADA) systems and industrial control systems (ICS); more accurately the payload specifically targeted PLCs controlling the centrifuges at the Iranian nuclear facility in Natanz. The worm's payload was able to physically damage the centrifuges by spinning them up and slowing them down to precisely the appropriate speeds for maximum degradation.[35] Although the full outcomes of the worm are unknown, it is known through satellite imagery that over one thousand centrifuges at the Natanz facility were destroyed.[36] This feat required some of the best programmers and ICS/PLC engineers in the world while leveraging a better understanding of the secretive Natanz facility layout than most of the engineers that worked at the facility would have had.[37]

Largely seen as a cyber weapon created and employed by at least one nation-state, Stuxnet launched intense discussions and multiple academic papers on the use of the cyberspace as a domain of warfare. The Russian Ambassador to NATO even went as far to state that the Stuxnet worm could have caused "a new Chernobyl" if the program would have released the Uranium gas in the centrifuges instead of causing degradation.[38] Though cyber operations had previously taken place in cyberspace, the media portrayal of the power of the Stuxnet cyber weapon made the discussion of cyber warfare a very public one. Stuxnet did for cyberspace what the early bombings in World War I did for airpower; it brought the discussion public and undoubtedly forced many corporations and nation-states to research more heavily into cyber capabilities. In a way, this event coupled with past cyber operations over the

last few decades including the 2007 cyber attacks against government and financial sectors in Estonia[39] and 2008 cyber attacks that coincided with the Russian invasion of Georgia[40] represents the start of the interim years of cyberspace.

Although Stuxnet was able to infect and spread to thousands of computer systems its only recognized targets were the centrifuges at Natanz. The event did not greatly impact systems in the US or reach the level of a cyber attack that pushed a nation into war. However, Secretary of Defense Leon Panetta stated, "The potential for the next Pearl Harbor could very well be a cyber attack."[41] Coupled with statements from General Alexander where he has stated that there are segments of the nation's critical infrastructure that are not currently prepared to handle cyber attacks, and that this worries him the most,[42] it is obvious that protecting these assets against cyber attacks is of paramount importance. Furthermore, Stuxnet has shown that these cyber capabilities exist and have been utilized by at least one nation-state.

The Stuxnet story is not over though. A piece of malware identified as Duqu was found on October 14th, 2011 and was quickly recognized as being related to the Stuxnet malware. Duqu is different from Stuxnet in that it is a targeted Remote Access Trojan (RAT) that steals information instead of a worm that damages centrifuges.[43] The RAT infected a number of different sites including universities, manufacturers, and certificate authorities in a style of attacks that would be used to make another Stuxnet styled cyber weapon.[44] Although different in style and targets, Duqu used much of the same source code from Stuxnet and the two have been linked as being made by the same coding team utilizing a common coding platform named Tilded.[45]

The Tilded platform has been described as being similar to a "lego set" where you can put together different pieces, or modules, of code to create entirely different malware.[46] This platform based approach allows a team to create a cyber weapon that can be quickly adapted to use different modules and payloads to be employed against very different targets while producing different outcomes. In addition, the malware created from the platform can be updated with different stealth measures including the changing of encryption algorithms used to hide its code as was done with an updated version of Duqu found in February, 2012.[47]

A platform based approach to weaponry is a direction that aerial warfare has been taking for years. Instead of creating aircraft with single functions, the DoD has purchased aircraft such as the F-16, F-22, and MQ-1 which can fulfill completely different mission sets based on the type of payload they are equipped with. This platform based approach is now evidently catching on in the cyberspace domain and poses a number of risks to various aspects of national security. A single cyber weapon platform could be responsible for stealing information from universities and manufacturers to create multiple

cyber weapons that would then attack aircraft, Internet nodes critical to command and control, air defense systems, and critical infrastructure.

General Norton Schwartz has stated that the Air Force is pursuing "cyber-methods to defeat aircraft" while other sources have indicated that the technology is already available.[48] Lt. Gen Herbert Carlisle stated, "The Russians and the Chinese have designed specific electronic warfare platforms to go after our high-value assets. Electronic attack can be the method of penetrating a system to implant viruses."[49] As traditional platform based weapon systems become more diverse and utilize more capabilities, such as advanced radar systems, they become more vulnerable to cyber attacks. These cyber vulnerabilities make the benefits of cyber weapon platforms more alluring to adversaries. The vulnerabilities combined with the capabilities demonstrated by the Tilded platform show that the threat of a future platform based cyber weapon system attacking multiple DoD and civilian sectors is not only possible but probable.

It is in these interim years of cyberspace that the government must reach out to civilian leadership in sectors such as critical infrastructure to ensure national security. Critical infrastructure operators, engineers, and developers offer keen insight into the systems that must be actively protected; yet they can only provide full details about their systems and their understanding of them when given actionable intelligence from the government. If presented with actionable cyber intelligence, declassified to the proper level, civilian counterparts can better advise how to defend systems they have been operating for years. While it makes sense to classify some cyber offensive capabilities it is likewise prudent to leave some cyber defense capabilities classified as well. Some cyber defenses though should be largely transparent so that weaknesses may be identified and remediated.[50]

Even non-cyber related ICS and SCADA system incidents have significant impacts that demonstrate the ability to drastically affect civilian populations. On 17 August 2009, the Shushenskaya dam, the largest in Russia with a height of 245m, experienced a non-cyber attack related incident which shook south central Siberia. A nine hundred and forty ton turbine was ripped apart with a sudden surge of water pressure that was the result in a fire at a power station over five hundred miles away. The incident resulted in the death of seventy-five people and $1.3 billion USD in rebuilding costs.[51] This incident was not related to a cyber attack nor was Shushenskaya the target of any nation-state; but the event represents an incident that could be carried out via a deliberately targeted cyber attack. If a similar incident was the result of a highly targeted attack the event could have had far more reaching impacts with increased civilian deaths and financial costs.

The Natanz nuclear enrichment facility and the Shushenskaya dam are only two examples of the uses of ICS and SCADA systems. These systems

affect every aspect of daily life including serving roles in the stock market, oil industry, electrical power grid, water filtration, and internet and satellite communication networks. ICS and SCADA systems are thus one of the most sought after and viable targets of nation-state based cyber weapons and must be treated accordingly. The protection of these systems is important in the evolution of the cyberspace domain, but the most important focus must be placed upon winning the domain in the long run. There is no better way to ensure the success of long term national security than the education of the next generation.

Winning the Next Generation

To be successful in the cyberspace domain, DoD and civilian partners must put emphasis on the education on the next generation. There are critical shortages in the availability of skilled cybersecurity professionals for jobs including investigative forensics and programming. The shortage makes filling jobs, such as those at the FBI Cyber Division, difficult.[52] The DoD also finds itself in a difficult position where the education of the next generation is concerned. NSA Director of Research and Development Dr. Michael Wertheimer briefed members of the U.S. Senate Armed Services Subcommittee the agency was having troubles recruiting and retaining professionals in the areas of computer science. He continued to state that seventy-seven percent of the information technology staff at the NSA resigns before retiring.[53] While the issue of making salaries competitive with the private industry may be one that needs addressed, the long term strategy must be one that learns from lessons taken from the aerial domain.

In the early days of airpower there was an excitement and sense of magic that surrounded airplanes and their pilots. The early pilots braved dangerous situations in a previously uncharted domain to break records and mesmerize crowds. The Reims Air Meet, which took place on 22 August 1909 in France, was the world's first major air show and opened the door for many more airshows to take place all around the globe.[54] These early men and women kept audiences captive at airshows and air races which not only inspired future pilots but educated the public on the capabilities of airpower.[55] Airshows gained even more attention in the time between World War I and World War II with the National Air Races; in 1929 a single airshow drew in more than a half a million people.[56]

In the 1920's there was a golden age and mysticism that surrounded flying. There existed a competition to fly higher, faster, and farther than anyone else. Three times between 1919 and 1921 the world altitude record was broken by Army pilots.[57] Cyber operators do not have to brave dangerous speeds and acrobatics as the early pilots did, but there is a real ability for cyber capabilities to captivate audiences and inspire the next generation of cyber operators.

Hacking and security conferences demonstrate the latest in security advancements, vulnerabilities, and exploits. The conferences also provide a way for those in attendance to network with people from a variety of backgrounds who all have a certain passion for cyberspace in common. Unfortunately though, these conferences are not as cheap as the early airshows or as embraced by the public. While some well-known conferences, such as DEF CON, cost as little as $150 USD to attend[58] others cost thousands of dollars to attend with optional training that is even more expensive.[59] Although these prices can be largely understood based on the type of audience the event is trying to reach as well as operation costs, there exists a problem with ever getting the mainstream public to attend cyberspace related conferences.

There are other conferences and advances in cyber related education that are orchestrated and benefit the domain. The Department of Defense Cyber Crime Center (DC3) hosts an annual cyber forensics challenge and convention that is a great opportunity to network, learn about the latest advances in technology, and sign up for training courses. The forensics challenge is free to compete in but the well-intended conference costs $500 USD to attend.[60] The Government and DoD must make larger strides in creating low cost conferences akin to airshows. At these conferences capabilities can be shown and cyberspace can be permitted an opportunity to create its own sense of magic and allure.

Retired vice chairman of the Joint Chiefs of Staff General James Cartwright, USMC, stated that some of the cyber offensive capabilities should be openly discussed and trained to in an effort to increase cyber deterrence.[61] Cyber conferences would be a perfect venue for members of the DoD to showcase some of the nation's cyber capabilities. This would have the benefit of attracting audiences and encouraging the next generation while deterring adversaries who would challenge the nation. In addition, cyber operators could give low cost, or possibly free, classes on the fundamentals of cybersecurity and hacking. These would offer fun and interactive ways to allow the next generation to become interested in the domain they will inherit.

Getting the youth educated and interested in cyber is incredibly important and an area where the nation is currently lacking. However, the DoD is taking steps in the right direction in its efforts to educate and train the generation of young leaders, officer and enlisted members alike, who have signed up to take part in the cyberspace domain. One prime example is the Air Force's Undergraduate Cyber Training (UCT) technical school located at Keesler AFB, MS. UCT opened June 21st, 2010 and offers cyber officers a six month training course which concludes with the students earning their Cyberspace Wings.[62] The schoolhouse fails students who do not pass the blocks of instruction offered and students are either retrained into new Air Force Specialty Codes (AFSCs) or cut from the Air Force.

The education offered at UCT is of high quality due largely to the faculty there. Much of the faculty is made up of Air Force enlisted and officer personnel who have first-hand experience and knowledge of cyberspace operations. These instructors work to inspire and train the next generation of cyberspace officers while fulfilling General Norton Schwartz's view that a successful career should include taking a tour of duty as an instructor.[63] Taking part as an instructor not only allows the faculty to sharpen their skills and academic pursuits but also to network and train with those that will be young leaders in their future squadrons. This networking creates a level of buy in from both the instructors and students and contributes to the overall cyber culture.

As instructors tell of their experiences and students become excited to create their own stories there is a level of passion that gets added to the domain. Instructor pilots and war veterans have the ability to inspire the next generation and so do the individuals that take part in various cyber missions.

The early culture surrounding airpower even supported acting in defiance towards superiors and non-flyers to gain favor and reverence amongst peers. Army Air Corps members would gain status in their groups by eliciting trouble and reprimand from Army leaders. They embraced being the outcasts and became empowered for it. They created a diverse group of individuals and culture that surrounded flying.[64] Military cyberspace professionals do not need to take such bold steps or challenge authority. The current military environment is favorable to the growth of the cyberspace domain and as stated previously there is not a need for an independent

cyber service like there was for airpower during the time of the Army Air Corps. However, the military cyberspace culture can feel very much like an outcast group owning to the fact that the domain is relatively new with unexplored and misunderstood capabilities.

The cyber culture already exists in its infancy and must be embraced instead of shunned. With a focus on education and the fostering of a competitive and rewarding instructor duty option for military members the cyber culture will grow and develop in its own right. The best cyberspace operators should compete for duty as an instructor and be rewarded with personal and career growing opportunities as a result. In this manner the education offered will continually be updated while invigorating the cyberspace operators who participate in it. Likewise, a strong and unique cyber culture will develop and inherently attract and keep passionate individuals dedicated to establishing cyber dominance.

Conclusion

Similarities between the traditional warfighting domains, especially the aerial domain, provide many lessons that leaders can use to guide the direction of cyberspace. However, the cyber domain is inherently different from the other domains of warfare as it is a manmade domain and as such can be drastically changed.[65] The infrastructure which comprises cyberspace can be modified and broken into a variety of networks as is apparent in the military's use of NIPR, SIPR, JWICS, and NSANet. By separating networks from other networks and websites, adding security protocols and authentication methods such as a CAC, and monitoring the networks for malicious network activity a network's security can be exponentially increased. This ability to change the cyberspace domain not only extends to the military's portion of the domain but to the cyberspace domain at the national level. Civilian infrastructure could also be separated out where networks that require more network security, an example being the financial sectors, could operate independently of the World Wide Web. Gateways between the World Wide Web and more secured networks would exist to provide access to everyone however at those gateways there could be additional layers of security to decrease the ability to perform malicious network activity.[66] The different options for the cyberspace domain in terms of physical infrastructure must be looked at and put under much scrutiny. However, this is not the focus of what the domain should look at currently.

The current focus for the cyberspace domain must be actionable cyber, the sharing of cyber intelligence, and education. Commanders must have knowledge of what they can request in terms of support from cyber operators that will directly benefit their missions. The reduction in overly classified information as it pertains to cyber intelligence and cyber capabilities will empower leaders at both the tactical, operational, and strategic levels. The declassified information can also be shared with civilian sectors to increase cyber awareness and the creation of meaningful defense strategies. This would bolster national security by allowing civilian leadership to help defend their sectors instead of solely relying on the DoD and DHS. Lastly, some cyber capabilities and cyber intelligence could be showcased at learning events and conferences. This would not only increase cyber deterrence to adversaries but inspire the next generation to take part in the cyberspace domain. The next generation must remain the long term strategy for protecting the domain and establishing cyber dominance.

As General Alexander stated, "If people who seek to harm us in cyberspace learn that doing so is costly and difficult, we believe we will see their patterns of behavior change. The technology is ready."[67] It is not only the technology that is ready. Interested parties throughout the cyberspace domain to include the DoD, civilian sectors, and the next generation are also ready for

the challenges ahead. Cyberpower is a powerful political and military tool that must be guided and its place in history cemented. The interim years of cyberspace are taking place now and leaders at all levels must act accordingly to ensure the success of the next era.

Notes

1. Alan Axelrod, *Little-known Wars of Great and Lasting Impact: The Turning Points in Our History We Should Know More About* (Beverly, MA: Fair Winds Press, 2009), 222.
2. D. Stevenson, *With Our Backs to the Wall: Victory and Defeat in 1918* (London: Penguin, 2012), 186.
3. Andreas Wittmer and Thomas Bieger, *Aviation Systems Management of the Integrated Aviation Value Chain* (Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 2011), 7.
4. The Official Web Site of the U.S. Air Force, "2nd Lt. Frank Luke Jr," 2 November 2010, http://www.af.mil/news/story.asp?storyID=123006460.
5. Lt Col Dr. James P. Tate (ret.), *The Army and its Air Corps: Army Policy Toward Aviation, 1919-1941* (Maxwell Air Force Base, AL: Air University Press, 1998), 33.
6. Capt B. Chance Saltzman and Thomas R. Searle, *Introduction to the United States Air Force* (Maxwell AFB, AL: Airpower Research Institute, College of Aerospace Doctrine, Research and Education and Air University Press, 2001), 6.
7. Lt Col Dr. James P. Tate (ret.), *The Army and its Air Corps: Army Policy Toward Aviation,* 62.
8. Pamela Feltus, "Mason Patrick and the Creation of the U.S. Air Corps," *U.S. Centennial of Flight Commission,* http://www.centennialofflight.gov/essay/Air_Power/Patrick/AP15.htm.
9. Lt Col Dr. James P. Tate (ret.), *The Army and its Air Corps: Army Policy Toward Aviation,* 67.
10. Ibid., 68.
11. Ibid., 190.
12. National Museum of the U.S. Air Force, "Brig. Gen. William 'Billy' Mitchell," 11 February 2010, http://www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=739.
13. Capt B. Chance Saltzman and Thomas R. Searle, *Introduction to the United States Air Force*, 12.
14. Ibid.
15. Col David A. Moore, *The Art of Aerial Warfare* (Maxwell Air Force Base, AL: Air University Press, 2005), 17.
16. Ibid., 19
17. Giulio Douhet, *The Command of the Air* (Washington, D.C.: Office of Air Force History, 1983), 9.
18. Col David A. Moore, *The Art of Aerial Warfare*, 68
19. Sir Stanley Baldsin, "A Fear for the Future," a speech to the British Parliament on 9 November 2011.

20. Giulio Douhet, *The Command of the Air,* 22-23.
21. Col David A. Moore, *The Art of Aerial Warfare*, 33.
22. John Stuart Mill, "The Contest in America," *Dissertations and Discussions* 1 (1868): 26.
23. David R. Mets, *The Air Campaign John Warden and the Classical Airpower Theorists* (Maxwell Air Force Base, AL: Air University Press, 1999), 39.
24. Benjamin S. Lambeth, "Airpower, Spacepower, and Cyberpower," In *Toward a theory of Spacepower: Selected Essays* edited by Charles D. Lutes, Peter L. Hays, Vincent A. Manzo, Lisa M. Yambrick, and M. Elaine Bunn (Washington, DC: National Defense University Press, 2011).
25. Joint Publication 5-0, *Doctrine for Joint Operations*, 11 August, 2011.
26. U.S. Army War College, *Campaign Planning Primer,* Department of Military Strategy, Planning, and Operations, AY 08.
27. Joint Publication 5-0, *Doctrine for Joint Operations*, 11 August, 2011.
28. Maj Eric D. Trias and Capt Bryan M. Bell, "Cyber This Cyber That, So What?" *Air and Space Power Journal* (Spring 2010): 90-100.
29. Joint Publication 5-0, *Doctrine for Joint Operations*, 11 August, 2011.
30. Carl von Clausewitz, Michael Howard, and Peter Paret, *On War* (Princeton, NJ: Princeton University Press, 1976), 101.
31. U.S. Department of Defense, "News Release: Cyber Command Achieves Full Operational Capability," *News Release*, 3 November 2010, http://www.defense.gov/releases/release.aspx?releaseid=14030.
32. Maj Gen Brett T. Williams, "Ten Propositions Regarding Cyberspace Operations," *Joint Force Quarterly*, no. 61 (2nd Quarter 2011): 10-17.
33. Gen Keith B. Alexander, “Building a New Command in Cyberspace,” *Strategic Studies Quarterly* 5, no. 2 (Spring 2011): 3–12.
34. Nicolas Falliere, Liam O Murchu, and Eric Chien, *W.32 Stuxnet Dossier*, Symantec White Paper (Symantec: Security Response, February 2011), 1-2. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
35. Ralph Langner, “*Stuxnet: A Deep Dive,”* 18 Jan 2012 video, http://www.digitalbond.com/2012/01/31/langners-stuxnet-deep-dive-s4-video/.
36. Yaakov Katz, "Stuxnet May Have Destroyed 1,000 Centrifuges at Natanz," *The Jerusalem Post*, 24 December 2010, http://www.jpost.com/Defense/Article.aspx?id=200843.
37. Ralph Langner, “*Stuxnet: A Deep Dive,”* 18 Jan 2012 video.
38. Ellen Messmer, "Stuxnet Could Have Caused ‘New Chernobyl,’ Russian Ambassador Says," *Network World*, 27 January 2011, http://www.networkworld.com/news/2011/012711-stuxnet-chernobyl.html.
39. Biony Kampmark, “Cyber Warfare Between Estonia and Russia,” *Contemporary Review* (Autumn, 2003): 288-293.
40. John Markoff, "Before the Gunfire, Cyberattacks." *The New York Times*, 12 August 2008. http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1
41. Jason Ryan, “CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor,” *ABC News,* 11 February 2011, http://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905#.T5M2ABHoK5I.

42. Charlie Rose, "Charlie Rose Talks to General Keith Alexander," *Businessweek,* 21 July 2011, http://www.businessweek.com/magazine/charlie-rose-talks-to-general-keith-alexander-07212011.html.
43. Boldizsar Bencsath, Gabor Pek, Levente Buttyan, and Mark Felegyhazi, *Duqu: A Stuxnet-like Malware Found in the Wild*, Laboratory of Cryptography and System Security Technical Report (Budapest University of Technology and Economics: Department of Telecommunications, October 2011), 6-7.
44. Symantec, "W32.Duqu: The Precursor to the Next Stuxnet," *Symantec Security Response*, 24 October 2011, http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet.
45. Kaspersky Lab, "Duqu and Stuxnet Not the Only Malicious Created by the Responsible Team," *Virus News*, 29 December 2011, http://www.kaspersky.com/about/news/virus/2011/Kaspersky_Lab_Experts_Duqu_and_Stuxnet_Not_the_Only_Malicious_Programs_Created_by_the_Responsible_Team.
46. Rob Waugh, "Lethal Stuxnet Cyber Weapon is 'Just one of Five' Engineered in Same Lab," *Daily Mail*, 29 December 2011, http://www.dailymail.co.uk/sciencetech/article-2079725/Lethal-Stuxnet-cyber-weapon-just-engineered-lab.html.
47. Greg Masters, "Duqu Variant Uncovered," *SC Magazine*, 23 March 2012, http://www.scmagazine.com/duqu-variant-uncovered/article/233385/.
48. TSgt Richard A Williams Jr., "CSAF Stresses Importance of Ready Future Force," *Official Site of the U.S. Air Force*, 24 February 2012, http://www.af.mil/news/story.asp?id=123291264
49. Eloise Lee, "Electronic Warfare Weapons," *Business Insider*, 15 March 2012, http://www.businessinsider.com/electronic-warfare-weapons-2012-3
50. Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (February 2012): 5-32.
51. Thomas Rid and Peter McBurney, "Cyber-Weapons," *The RUSI Journal* 157, no.1 (February/March 2012), 6-13
52. Kevin Coleman, "United States at Risk from Shortage of Trained Cybersecurity Professionals," *Defense Systems*, 22 June 2011, http://defensesystems.com/articles/2011/06/08/digital-conflict-cyber-worker-shortage.aspx.
53. Brian Donohue, "Experts Tell Senate: Government Networks Owned, Resistance Is Futile," *Threatpost*, 21 March 2012, http://threatpost.com/en_us/blogs/experts-tell-senate-government-networks-owned-resistance-futile-032112.
54. David H. Onkst, "Explorers, Daredevils, and Record Setters: An Overview," *U.S. Centennial of Flight Commission,* http://www.centennialofflight.gov/essay/Explorers_Record_Setters_and_Daredevils/EX_OV.htm.
55. David H. Onkst, "The First U.S. Airshows - the American Air Meets of 1910," *U.S. Centennial of Flight Commission,* http://www.centennialofflight.gov/essay/Explorers_Record_Setters_and_Daredevils/Early_US_shows/EX4.htm.
56. David H. Onkst, "Air Shows - An International Phenomenon," *U.S. Centennial of Flight Commission,* http://www.centennialofflight.gov/essay/Social/airshows/SH20.htm..

57. Lt Col Dr. James P. Tate (ret.), *The Army and its Air Corps: Army Policy Toward Aviation,* 27.
58. DEF CON, "Official DEF CON FAQ," https://www.defcon.org/html/links/dc-faq/dc-faq.html.
59. Hacker Halted, "Registration," http://www.hackerhalted.com/2011/Registration.aspx.
60. DoD Cyber Crime Conference, "Registration," http://www.dodcybercrime.com/12CC/register.asp.
61. Andrea Shalal-Esa, "Ex-U.S. General Urges Frank Talk on Cyber Weapons," *Reuters,* 6 November 2011, http://uk.reuters.com/article/2011/11/06/us-cyber-cartwright-idUKTRE7A514C20111106?mid=520.
62. Bruce Rolfsen, "3,000 Officers Switch to Cyberspace Specialty," *Air Force Times*, 17 May 2010, http://www.airforcetimes.com/news/2010/05/airforce_cyber_careers_051710/
63. Gen Norton A. Schwartz, Chief of Staff. To all Airmen. Memorandum, 8 March 2012.
64. Lt Col Dr. James P. Tate (ret.), *The Army and its Air Corps: Army Policy Toward Aviation,* 192.
65. Maj Gen Brett T. Williams, "Ten Propositions Regarding Cyberspace Operations."
66. Richard A. Clarke and Robert K. Knake, *Cyber War* (NY: HarperCollins, 2010), 161.
67. Gen Keith B. Alexander, "Building a New Command in Cyberspace."

1st Lieutenant Robert M. Lee is stationed in Germany working under the Air Force Intelligence, Surveillance, and Reconnaissance Agency. He is a graduate of the United States Air Force Academy and of the Air Force's Undergraduate Cyber Training technical school. Lt Lee has published and presented internationally on topics including control systems cyber security, cyber warfare, advanced cyber threats, and future nation-state cyber weapons.